HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Kurzfassung der Diplomarbeit

Abteilung	**I**
Name der Diplomandin / des Diplomanden	**Christoph Bösch** **Marco Ott**
Diplomjahr	**2003**
Titel der Diplomarbeit	**Security Visualizer**
Examinator / Experte	**Prof. Dr. Peter Heinzmann / Dr. Th. Siegenthaler, CSI**
Industriepartner	**Swisscom Enterprise Solutions, Thomas Amrein**

Ausgangslage: Managed Security Service Provider (MSSP) wie Swisscom Enterprise Solutions bieten ihren Kunden (KMU, Schulen usw.) eine sichere Verbindung mit dem Internet an. Zur Überwachung dieser Verbindung wird unter anderem das Intrusion Detection System Snort eingesetzt.
Da die von Snort gesammelten Daten schwierig zu interpretieren sind, sollen sie in einer für den Kunden verständlichen Form visualisiert werden. Zusätzlich zu den Übersichtsdarstellungen sind auch Drill-Down- und Baselining-Funktionen erwünscht.

Ergebnis: Ein Ziel der Arbeit war, ein in sich abgeschlossenes System zu entwickeln, welches einem MSSP ermöglicht, Sensor-Module für die Datensammlung mit Snort und die entsprechenden Reporting-Module für die Darstellung dieser Daten flexibel einzusetzen. Als Plattform für diese Module hätten ursprünglich Sun/Solaris-Systeme verwendet werden sollen. Da der Industriepartner diese jedoch nicht rechtzeitig zur Verfügung stellen konnte, verschob sich das Schwergewicht der Arbeit auf die Aufbereitung, Darstellung und Interpretation der Snort-Daten. Das im Rahmen der Diplomarbeit realisierte System ermöglicht die webbasierte Darstellung der Snort-Daten in diversen Formen. Es bietet Zugang zu Detailinformationen sowie Vergleiche zwischen verschiedenen Sensor-Modulen. Im Theorieteil der Arbeit wurden Grundlagen der eingesetzten Technologien sowie das Thema „Attacken“ abgehandelt.

Fazit: Dem Industriepartner Swisscom steht mit dem Security Visualizer ein System zu Verfügung, mit welchem Snort-Daten abstrahiert von der darunterliegenden Technik dargestellt werden können. Die Managed Security Service Provider (MSSP) Kunden können sich dank dem Security Visualizer schnell einen Überblick über die Sicherheit und Verwundbarkeit ihrer Netze verschaffen.